B1

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 140 013
B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: 19.07.89

(51) Int. Cl.⁴: G 07 F 7/10, H 04 L 9/02

(21) Application number: 84110268.4

(22) Date of filing: 29.08.84

(54) Improvements in point of sale and electronic funds transfer systems.

(30) Priority: 17.09.83 GB 8324917

(43) Date of publication of application:
08.05.85 Bulletin 85/19

(45) Publication of the grant of the patent:
19.07.89 Bulletin 89/29

(84) Designated Contracting States:
CH DE FR GB IT LI NL SE

(56) References cited:
EP-A-0 055 986
GB-A-2 050 021
GB-A-2 060 233

IBM TECHNICAL DISCLOSURE BULLETIN, vol. 24, no. 7B, December 1981, pages 3906-3909, New York, US; R.E.LENNON et al.: "Pin protection/verification for electronic funds transfer"

(73) Proprietor: International Business Machines Corporation
Old Orchard Road
Armonk, N.Y. 10504 (US)
(84) CH FR GB IT LI NL SE

(73) Proprietor: IBM United Kingdom Limited
P.O. Box 41 North Harbour
Portsmouth Hampshire PO6 3AU (GB)
(84) GB

(73) Proprietor: IBM DEUTSCHLAND GMBH
Pascalstrasse 100
D-7000 Stuttgart 80 (DE)
(84) DE

(72) Inventor: Brachtl, Bruno
Weinbergstrasse 20
D-7033, Herrenberg 1 (DE)
Inventor: Holloway, Christopher J.
13 Wilders Close
Woking Surrey GU21 3HA (GB)
Inventor: Lennon, Richard Edward
6222 Mount Airy Road
Saugerties New York 12477 (US)
Inventor: Matyas, Stephen Michael
Rd 5, Box 19F
Kingston New York 12401 (US)

Courier Press, Leamington Spa, England.

EP 0 140 013 B1

(72) Inventor: Meyer, Carl Heinz-Wilhelm
27 Norma Court
Kingston New York 12401 (US)
Inventor: Oseas, Jonathan
147 Hurley
New York 12443 (US)

(74) Representative: Appleton, John Edward
IBM United Kingdom Limited Intellectual
Property Department Hursley Park
Winchester Hampshire SO21 2JN (GB)

Description

Field of the invention

This invention relates generally to point of sale and electronic funds transfer systems and in particular to the personal verification of users of such systems.

Electronic funds transfer (EFT) is the name given to a system of directly debiting and crediting customer and service suppliers' accounts at the instant of confirmation of a transaction. The accounts are held at a bank, or credit card company's central processing system, which is connected to a dedicated network of retailers or service suppliers' data processing equipment. In this way no cash or check processing is required for the transaction.

Point of sale (POS) is the name given to retailers' data processing systems in which check-out or sale point tills are connected directly to a data processing system. Details of current transactions can then be used for stock control, updating customer accounts held locally and monitoring the retailers flow of business. A POS terminal can include the function required for an EFT terminal and be connected to an EFT network as well as the local retailers data processing system.

In a simple application each bank or credit card company has its own network and each customer of the bank has a credit card which can only be used on that network, such a network is described in European Patent Publication 32193.

Background of the invention

European Patent Publication 32193 (IBM Corporation) describes a system in which each user and retailer has a cryptographic key number—retailer's key Kr and user's key Kp—which is stored together with the user's account number and retailer's business number in a data store at the host central processing unit (cpu). The retailer's key and the user key are used in the encryption of data sent between the retailer's transaction terminal and the host cpu. Obviously only users or customers with their identity numbers and encryption keys stored at the host cpu can make use of the system. As the number of users expands there is an optimum number beyond which the time taken to look up corresponding keys and identity numbers is unacceptable for on-line transaction processing.

The system described is only a single domain and does not involve using a personal identification number (PIN). Verification of the user's identity is at the host and without a PIN there is no bar to users using stolen cards for transactions.

European Patent Publication 18129 (Motorola Inc.) describes a method of providing security of data on a communication path. Privacy and security of a dial-up data communications network are provided by means of either a user or terminal identification code together with a primary cipher key. A list of valid identification codes and primary cipher key pairs is maintained at the central processing unit. Identification code and cipher key pairs sent to the cpu are compared with the stored code pairs. A correct comparison is required before the cpu will accept encoded data sent from the terminal. All data sent over the network is ciphered to prevent unauthorised access using the relevant user or terminal key.

The system described is a single domain in which all terminal keys (or user keys) must be known at a central host location. Hence, the ideas described in the patent do not address a multi-host environment and thus are not addressing the interchange problem either.

UK Patent Application 2,052,513A (Atalla Technovations) describes a method and apparatus which avoids the need for transmitting user-identification information such as a personal identification number (PIN) in the clear from station to station in a network such as described in the two European Patent Publications mentioned above. The PIN is encoded using a randomly generated number at a user station and the encoded PIN and the random number are sent to the processing station. At the processing station a second PIN having generic application is encoded using the received random number and the receive encoded PIN and the generic encoded PIN are compared to determine whether the received PIN is valid.

This system does not use a personal key and as a consequence for a sufficiently cryptographically secure system, it is necessary to have a PIN with at least fourteen random characters (four bits each). This is a disadvantage from the human factor point of view as users will have difficulty remembering such a long string of characters and the chances of inputting unintentionally an incorrect string is very large. If a phrase, which a user can easily remember, is employed for a PIN, about 28 characters are required. Although remembering the information is not a problem, inputting such a long string of data still presents a human factors problem.

The EFT system made possible by the systems described in the above patent applications is limited to a single host cpu holding the accounts of all users, both retailers and customers.

An EFT system in which many card issuing organisations (banks, credit card companies, etc.) are connected and many hundreds of retail organisations are connected through switching nodes such as telephone exchanges, brings many more security problems.

PCT publication Wo 81/02655 (Marvin Sendrow) describes a multi-host, multi-user system in which the PIN is ciphered more than once at the entry terminal. The data required to validate and authorise the transactions is transmitted to a host computer which accesses from its stored data base the data that is required to decipher and validate the transaction, including the ciphered PIN. A secret terminal master key must be maintained at each terminal. A list of these master keys is also maintained at the host computer.

The maintaining of lists of terminal master keys at each of the card issuing organisation's host computers is obviously a difficult task, in a complex system where the terminal keys are not controlled and, therefore, not known by the card issuing host.

European Patent Publication 55580 (Honeywell Information Systems) seeks to avoid the necessity of transmitting PIN information in the network by performing PIN verification at the entry point terminal. This is achieved by issuing each user with a card that has encoded in the magnetic stripe the bank identification (BIN), the user's account number (ACCN) and a PIN offset number. The PIN offset is calculated from the PIN, BIN and ACCN. The user enters the PIN at a keyboard attached to the terminal, which also reads the PIN offset, BIN and ACCN from the card. The terminal then re-calculates a PIN offset from the user's entered PIN, the BIN, and ACCN. If the re-calculated PIN offset is the same as the PIN offset read from the card then verification of the PIN is assumed. This approach has the disadvantage in that the system is not involved in the validation and that knowing that the PIN offset is calculated from the PIN, the BIN and ACCN, anyone having knowledge of the process can manufacture fraudulent cards with valid PINS.

UK Patent Application 2050021A (Atalla Technovations) describes a secured data Transmission system that relies upon the favourable comparison of coded signals derived from information about authorised users and data terminals. The authorisation is pre-started and subsequently supplied under manual commands to generate an operating key which is then used to encode and decode data that is entered after an initialisation procedure.

Advances in microcircuit chip technology has now led to the possibility that user cards instead of having user data stored on a magnetic stripe can contain a microprocessor with a read only store (ROS). The microprocessor is activated when the card is placed in an EFT terminal and the appropriate power and data transmission interface connections are made. The microprocessor on the card is controlled by control programs stored in the ROS. The users and issuers identification can also be stored in the ROS together with other information.

Examples of such cards including a microprocessor are shown in United Kingdom Patent Applications 2,081,644A and 2,095,175A.

European Patent Application No. 82306989.3 (IBM) describes a method and apparatus for testing the validity of personal identification numbers (PIN) entered at a transaction terminal of an electronic funds transfer network in which the PIN is not directly transmitted through the network. The PIN and the personal account number (PAN) are used to derive an authorisation parameter (DAP). A unique message is sent with the PAN to the host processor where the PAN is used to identify a valid authorisation parameter (VAP). The VAP is used to encode the message and the result (a message authentication code MAC) transmitted back to the transaction terminal. The terminal generates a parallel derived message authentication code (DMAC) by using the DAP to encode the message. The DMAC and MAC are compared and the result of the comparison used to determine the validity of the PIN.

In such a system the generation of DAP as well as VAP is based on a short PIN only and is therefore cryptographically weak. Furthermore, the EFT transaction terminal has access to all the information carried on the identity card which may be regarded as a security weakness in the system. The present invention seeks to overcome such deficiencies by storing personal key data in a portable personal processor carried on a card and only processing the key data on the card.

In any multi-domain communication network where such domain includes a data processor and in which cryptographically secure transmission takes place it is necessary to establish cross domain keys. A communication security system in which cross domain keys are generated and used is described in United States Patent No. 4,227,253 (IBM). The patent describes a communication security system for data transmissions between different domains of a multiple domain communication network where each domain includes a host system and its associated resources of programs and communication terminals. The host systems and communication terminals include data security devices each having a master key which permits a variety of cryptographic operations to be performed.

When a host system in one domain wishes to communicate with a host system in another domain, a common session key is established at both host systems to permit cryptographic operations to be performed. This is accomplished by using a mutually agreed upon cross-domain key known by both host systems and does not require each host system to reveal its master key to the other host system. The cross domain key is enciphered under a key encrypting key at the sending host system and under a different key encrypting key at the receiving host system. The sending host system creates an enciphered session key and together with the sending cross-domain key performs a transformation function to re-encipher the session key under the cross domain key for transmission to the receiving host system. At the receiving host system, the receiving host system using the cross-domain key and the received session key, performs a transformation function to re-encipher the received session key from encipherment under the cross domain key to encipherment under the receiving host system master key. With the common session key now available in usable form at both host systems, a communication session is established and cryptographic operations can proceed between the two host systems.

Reference to the following publications are included as giving general background information is encryption techniques and terminology:

1. IBM Technical Disclosure Bulletin, Vol. 19, No. 11, April 1977, p. 4241, "Terminal Master Key Security" by S. M. Matyas and C. H. Meyer.

2. IBM Technical Data Bulletin, Vol. 24, No. 1B, June 1981, pp. 561—565, "Application for Personal Key Crypto with Insecure Terminals" by R. E. Lennon, S. M. Matyas, C. H. Meyer and R. E. Shuck;
3. IBM Technical Data Bulletin, Vol. 24, No. 7B, December 1981, pp. 3906—3909, "Pin Protection/ Verification for Electronic Funds Transfer' by R. E. Lennon, S. M. Matyas and C. H. Meyer;
4. IBM Technical Disclosure Bulletin, Vol. 24, No. 12, May 1982, pp. 6504—6509, "Personal Verification and Message Authentication Using Personal Keys" by R. E. Lennon, S. M. Matyas and C. H. Meyer;
5. IBM Technical Disclosure Bulletin, Vol. 25, No. 5, October 1982, pp. 2358—2360, "Authentication with Stored KP and Dynamic PAC" by R. E. Lennon, S. M. Matyas and C. H. Meyer.

Summary of the invention

The present invention uses a time variant key which is based upon a card users personal account number (PAN), personal key (KP) and a transaction variable. When an issuer host receives a message including a message authentication code generated using the time variant key (identified as KSTR1 in the preferred embodiment) then the issuer is assured that when the message was formed then a user with a valid PAN and a valid KP was involved and that the message does not originate from a potentially fraudulent source.

Another source of fraudulent attack is guarded against by the encipherment of the transaction variable under the key KS and using this quantity in the calculating of the message authentication code. When a message is received by the issuer including the session key enciphered under a cross-domain key then if the enciphered session key has been changed for any reason, the message authentication code calculated on the changed session key will not be the same as the received message authentication code (MAC). This MAC check therefore not only validates the part of the message in which the MAC was calculated, but also the correct reception of the enciphered session key.

The use of the transaction variable generated at the EFT terminal and the personal key (KP) held only on the card also ensures that the transaction variable cannot be produced separately by a potentially fraudulent user, terminal operator or even a potentially fraudulent issuer.

According to the invention there is provided an electronic funds transfer system in which EFT terminals are connected through a local data processing centre (acquirer) to a public switch system (switch), a plurality of card-issuing agencies' data processing centres are also connected to the public switch system and each user of the EFT system has a personal secure intelligent bank card on which is stored a personal account number (PAN) and a personal key (KP), the system including means at eahc local data processing centre to generate session keys (KS) for each of its locally attached terminals, and to transmit an associated session key to a respective terminal, at each terminal means to store the session key, means to encipher sensitive data (PAN) under the session key whenever a transaction request message is generated, means to generate a transaction variable for each transaction initiated at the terminal and to transfer the transaction variable to the card, means to transfer a message request including the transaction variable enciphered under KS to the users card and means on the card to generate a message authentication code using a time-variant key (KSTR1) based upon the users PAN, KP and the transaction variable, means at each local data processing centre to encipher the appropriate session key under a cross-domain key whenever a transaction request message is received and to add the enciphered key to the message, means at each processing node of the public switch system to translate the enciphered session key from encipherment under a received cross-domain key to a transmission cross-domain key, means at the card issuing agency's data processing centre to decipher the enciphered session key and to use the key to decipher any sensitive data contained in the request message, and means to regenerate the message authentication code using KSTR1 which is generated from parameters based upon the PAN and KP and the received transaction variable for comparison with the message authentication code included in the received message.

In order that the invention may be fully understood a preferred embodiment thereof will now be described with reference to the accompanying drawings:

Brief description of the drawings

Fig. 1 is a block schematic showing the component parts of an EFT network;
Fig. 2 is a block schematic of the retail store components of the EFT network;
Figs. 3—9 illustrate enciphering techniques used in the preferred embodiment;
Figs. 10—12 are flow charts illustrating the steps of the method of the preferred embodiment;
Figs. 13—17 illustrate the message formats used in the preferred embodiments.

Table of abbreviations

In the designation of the preferred embodiment, the following abbreviations are used:

AP=authentication parameter (generated from PAN, KP and PIN)
BID=bank or card issuer's identity
KI=interchange key
KP=personal key
KM0=host master key
KM1=first variant of host master key

KM2=second variant of host master key
KM3=third variant of host master key
KMT=terminal master key
KS=session key
KST1=transaction session key one (generated from Tterm, card and KTR1)
KSTR2=transaction session key two (randomly or pseudo-randomly generated)
KSTR3=transaction session key three (generated from Tiss, term, card and KTR2)
KTR1=transaction key one (generated from PAN and KP)
KTR2=transaction key two (generated from PAN, KP and PIN)
MAC=message authentication code
PAN=primary account number
PIN=user's personal identification number
Tcard=time-variant information generated by bank card
Tiss=time-variant information generated by issuer
Tterm=time-variant information generated by terminal
Tterm,card=time-variant information generated from Tterm and Tcard using a one-way function
Tiss,term,card=time-variant information generated from Tiss and Tterm,card
TAP1=time-variant authentication parameter (generated from Tterm,card and AP)
TAP2=time-variant authentication parameter (generated from Tiss,term,card and TAP1
TID=terminal ID
SEQterm=terminal sequence number
SEQiss=issuer sequence number.

Preferred embodiment of the invention

Referring now to Figure 1 an EFT network is shown in which card issuing agencies' data processing centres 10 are connected through a packet switched communication network 12 through network nodes 14 to retail store controllers 16. Each store controller 16 is connected directly to the store's EFT transaction terminals 18 which have an interface including power and input-output means for communicating with a portable microprocessor 20 contained on a personal identity card issued by one of the card issuing agencies.

The store controller 16 may also be directly connected with the retailers own data processing centre 22.

The retail store components of the network are expanded in Fig. 2. The EFT transaction terminal may include a point of sale checkout terminal 24 including an EFT module 26 and having a consumer module 28 connected so that a user can key-in data on the module. The store computers can also include an enquiry station which is an EFT module 30 and consumer module positioned so that users can communicate directly with the card issuing agency asking for example for the current balance or credit limit on their accounts before making a purchase.

The consumer modules 28 are a twelve button key pad with, for example, a liquid crystal display such as are now in common use for other applications, hand calculators, remote TV selectors, etc.

The EFT modules and point of sale terminals each have their own microprocessor and encryption-decryption modules together with read only and random access storage devices. The network nodes have a larger capacity processor such as the IBM Series 1 processing unit, (IBM is a Registered Trade Mark).

In the preferred embodiment of the invention a card issuing agency prepares individual user cards for each user. The cards include a personal portable microprocessor, a read only store (ROS) a random access memory (RAM) and an encryption device. The ROS for each user includes a personal encryption key (KP) a user identity code or personal account number (PAN) and a card issuer's identity code (BID). The KP, and PAN, are also stored at the issuing agency's data processing centre together with a personal identification number (PIN). BID is a code that identifies the issuing agency's data processing centre to the EFT network.

Each unit in the network has an identity code which is used for routing messages through the network.

The EFT modules also include a microprocessor, RAM and ROS stores and an encryption device. Depending upon the further encryption techniques employed in the network, the store controllers and packet switched network nodes contain data processing and encryption devices.

When the EFT network is set up in order for secure transmission of transaction messages to take place it is necessary to generate identity numbers and encipherment keys used at the various nodes of the network. These pregenerated quantities are:

AP—generated at card issuing agency; defined as: $E_{PIN \oplus KP}(PAN) \oplus PAN$.
KI—generated at switch; issuer, acquirer
KP—generated at issuing agency;
KM0—generated at issuer, acquirer, switch
KMT—generated at acquirer
KTR1—generated at issuer; defined as: $D_{KP}(PAN) \oplus PAN$.
KTR2—generated at issuer; defined as: $D_{PIN \oplus KP}(PAN+1) \oplus (PAN+1)$.
PAN—generated at issuer
PIN—generated at issuer
TID—generated at acquirer.

Where ⊕ denotes modulo 2 addition and + denotes modulo 2^{64} addition.

At initialisation of the system the KP, PIN and PAN quantities are used to generate AP, KTR1 and KTR2, which are unique to each user card. The quantities AP, KTR1 and KTR2 are stored at the issuer's data processing centre enciphered under the second variant (KM2) of the issuer's master key and associated together and enclosed by the PAN for the user. The quantities PAN, PIN and KP for each user are also stored offline for backup purposes (e.g., in a safe or vault) and are erased from main memory once AP, KTR1 and KTR2 have been generated.

For each card, a unique PAN and KP are stored in the cards ROM.

Each user must store separately or remember the unique PIN.

A unique TID and KMT are stored in each terminal and at the associated acquirer.

A unique KM0 for each processing node is stored at that node, i.e., issuer, acquirer and switch.

During the course of a transaction, some of these values and others based upon stored values are generated dynamically at locations in the network.

The Fig. 1 configuration of the system shows a complete organisation in which a large retail outlet has its own "in-store" data processing system. In this case, the retailer's data processing system is regarded as the acquirer and the PSS node as the switch.

In a simpler organisation where a small retailer may have only one terminal connected directly to the PSS node, then the function of the acquirer and switch are combined and there is no cross-domain translation required between acquirer and switch.

The following cryptographic operations are available at the host system of the issuer, acquirer and switch.

Encipher Data (ECPH):

ECPH: $[E_{KM0}K, X_1, X_2, \ldots, X_n]$
$\rightarrow E_K X_1, E_K(X_2 \oplus E_K X_1), \ldots, E_K(X_n \oplus E_K X_{n-1})$

Decipher Data (DCPH):

DCPH: $[E_{KM0}K, Y_1, Y_2, \ldots, Y_n]$
$\rightarrow D_K Y_1, D_K(Y_2) \oplus Y_1, \ldots, D_K(Y_n) \oplus Y_{n-1}$

Set Master Key [SMK]:

SMK: [KM0] Write Cipher Key KM0 in Master Key Storage

Encipher Under Master Key (EMK0):

EMK0: $[K] \rightarrow E_{KM0}K$

Re-encipher From Master Key (RFMK):

RFMK: $[E_{KM1}KN, E_{KM0}K] \rightarrow E_{KN}K$

Re-encipher To Master Key (RTMK):

RTMK: $[E_{KM2}KN, E_{KN}K] \rightarrow E_{KM0}K$

Translate Session Key (TRSK):

TRSK: $[E_{KM3}KN1, E_{KN1}KS, E_{KM1}KN2] \rightarrow E_{KN2}KS$

European Patent Application 821108/49 describes a system for performing the TRSK function.

The following cryptographic operations are available at the terminal:

Load Key Direct (LKD):

LKD: [K] Load Cipher Key K into Working Key Storage

Write Master Key (WMK):

WMK: [KMT] Write Cipher Key KMT In Master Key Storage

Decipher Key (DECK):

DECK: $[E_{KMT}K]$ Decipher $E_{KMT}K$ under the terminal master key KMT and load recovered cipher key K into the Working Key Storage

Encipher (ENC):

ENC: $[X_1, X_2, \ldots, X_n]$
$\rightarrow E_{KW}X_1, E_{KW}(X_2 \oplus E_{KW}X_1), \ldots, E_{KW}(X_n \oplus E_{KW}(X_{n-1}))$

Where KW is the current working key in the working key storage.

Decipher (DEC):

DEC: $[Y_1, Y_2, \ldots, Y_n]$
$\rightarrow D_{KW}(Y_1), D_{KW}(Y_2) \oplus Y_1, \ldots, D_{KW}(Y_n) \oplus Yn-1$

Where KW is the current working key in the working key storage.

Encipher Data (ECPH):

ECPH: $[E_{KMT}K, X_1, X_2, \ldots, X_n]$
$\rightarrow E_K(X_1), E_K(X_2 \oplus E_K(X_1)), \ldots, E_K(X_n \oplus E_K(X_{n-1}))$

Decipher Data (DCPH):

DCPH: $[E_{KMT}K, Y_1, Y_2, \ldots, Y_n]$
$\rightarrow D_K(Y_1), D_K(Y_2) \oplus Y_1, \ldots, D_K(Y_n) \oplus Y_{n-1}$.

At this point it is useful to realise that quantities held at the issuer are stored enciphered under the processor master key KM0 or a master key variant KM2. The general decipher-encipher sequence is illustrated in Fig. 3. A sensitive quantity (Q) is held in store enciphered under KM2 ($E_{KM2}Q$). The enciphered value is deciphered using KM2 as the key and Q is used as the key to decipher a further variable KEY stored enciphered under key Q (E_QKEY). The deciphered KEY is then enciphered using the master key KM0 as the key and the result is $E_{KM0}(KEY)$. This first operation is called a RTMK function.

To use KEY to encipher a further quantity Q2 then $E_{KM0}KEY$ is deciphered using KM0 as the key and the deciphered KEY is used as the key in enciphering Q2 giving $E_{KEY}Q2$. This second operation is called an ECPH function.

These operations all take place in the cryptographically secure hardware circuits (defined cryptographic facility or security module) and consequently while Q and KEY appear in the clear, they are not available outside the secure hardware.

Fig. 4 illustrates the RFMK sequence. A key KI stored enciphered with KM1 as $E_{KM1}(KI)$ is deciphered using KM1 as the key recovering KI in the clear. A second key KEY stored under encipherment of KM0 as $E_{KM0}KEY$ is deciphered using KM0 as the key. The result of this decipherment (KEY) is then enciphered using KI as the key giving $E_{KI}KEY$.

As part of the system initialisation process, the acquirer (or other node) generates a series of terminal master keys (KMTi) for all the terminals associated with the acquirer system. These keys are protected by being enciphered under the first variant (KM1acq) of the acquirer master key (KMØacq) by an Encipher Master Key function (EMK1) to produce the result set forth by the following notation:

EMK1: $[KMTi] \rightarrow E_{KM1acq}KMTi$.

The enciphered terminal keys are stored at the acquirer in a cryptographic data set until required for use in a cryptographic operation. Each terminal stores its own KMTi generated by the acquirer in a secure store.

When a session is to be established between the acquirer and a requesting terminal, it is necessary to establish a common session key (KS) between the acquirer and the terminal for secure data communication. Thus, the acquirer causes a pseudo random or random number to be generated which is defined as being the session key enciphered under a secondary file key KNFacq, i.e., $E_{KNFacq}KS$ and is retained at the acquirer for cryptographic operations during the communication session. In order to securely distribute the session key to the requesting terminal, the acquirer performs a transformation function which re-enciphers the session key from encipherment under the acquirer secondary file key to encipherment under the terminal master key, i.e., from $E_{KNFacq}KS$ to $E_{KMTi}KS$. This transformation function may be defined by the notation:

TRSK: $[E_{KMH3acq}KNFacq, E_{KNFacq}KS, E_{KMH1acq}KMTi] \rightarrow E_{KMTi}KS$

Since KS is now enciphered under KMTi, it may be transmitted over the communication line to bind the requesting terminal to the acquirer for a communication session.

When the EFT network is set up and the initialisation is complete, i.e., the pregenerated values are stored at the respective locations, EFT transactions may occur. Each terminal has a sequence number counter which provides SEQterm for each transaction message initiated at that terminal. Each host also has a sequence number counter which provides SEQiss for each transaction message (Mresp) generated at the host data processing centre. These SEQ numbers are provided for audit purposes and do not relate directly to the invention.

The preferred method of testing the validity of messages in the network is as follows:

A transaction is initiated at a POS terminal when a customer's user card is inserted in the EFT module. Insertion of the card couples the power and data bus connections to the personal portable microprocessor (p.p.m.).

At the ppm (20 Fig. 1):

Step C1 Generate Tcard and transfer this variable to the EFT terminal together with card issuer identification (BID), personal account number (PAN). Other information such as credit limit may be passed at this time.

Tcard is a time variant quantity and the method employs a system of time variant quantities in contrast to a universal time reference such as a time-of-day clock. This approach avoids synchronisation problems among the several generators of the desired time-variant information. Each node (ppm (20), EFT terminal (18) and card issuer host (10)) generates its own time variant quantity, Tcard, Tterm and Tiss, respectively. (If desired, time-of-day clock values may be included for auditing purposes).

At the different nodes time variant quantities are obtained by combining various ones of the three individual quantities using an encipher function.

At the EFT terminal (18 Fig. 1):

Step T1 Generate Tterm and the combined Tterm,card based upon Tcard and Tterm. The generation of Tterm,card is illustrated in Fig. 5. The variable Tcard is ciphered using the variable Tterm as an encryption key. To accomplish this Tterm is loaded as the working key using a Load Key Direct (LKD) operation and then Tcard is enciphered under Tterm using an Encipher (ENC) operation, as follows:

LKD: [Tterm] load Tterm as the working key.

ENC: [Tcard]$\rightarrow E_{Tterm}$Tcard.

The result, i.e., E_{Tterm}(Tcard) is referred to as Tterm,card and stored in the terminals RAM.

Step T2 Receive and store other transaction data (Card issuing agency BID, PAN, etc.).

Step T3 Formulate a message request (Mreq) having a format shown in Fig. 13 which at this time includes the combined time variant data Tterm,card generated at the terminal, the stored card information, TID and other transaction data.

The Mreq is formed in a buffer store portion of the terminals RAM and includes message address information BID.

Step T4 Transfer the transaction request (TR) portion of Mreq and Tterm to the personal portable microprocessor.

At the ppm:

Step C2 Using the received Tterm generate Tterm,card of reference using the technique shown in Fig. 5.

Step C3 Generate and store a transaction session key (KSTR1) using KP and Tterm,card. KSTR1 is used as the end to end key between the card and the issuer and is generated from PAN and KP read from the card and the card generated (Step T2) Tterm,card.

The generation of KSTR1 is illustrated in Fig. 6. Using the user's personal key (KP) as the key the PAN is deciphered and then exclusively OR'd with the result to produce a time invariant transaction key KTR1. Tterm,card is then deciphered using KTR1 as the key to produce the first transaction session key KSTR1.

Step C4 Store in the ppm RAM both KSTR1 and Tterm,card.

Step C5 Compute a message authentication code (MAC1 card, iss,) on the TR portion of Mreq which will include Tterm,card and using KSTR1.

The generation of a message authentication code (MAC), which uses the Encipher Data (ECPH) operation, is illustrated in Fig. 7. The method used is the standard cipher block chaining (CBC) mode of DES. The inputs defined as X1, X2, . . ., Xn are 64 bit blocks of the request message. The initialising vector ICV is set equal to zero in this process.

The result of the first XOR is then enciphered under the key K. In Step C5 the key K=KSTR1 is used. The second block X2 is then XOR'd with the result of the first encipherment and the output of this XOR is enciphered using key K. This process is continued until Xn is reached and the output or part thereof is defined as the MAC.

Step C6 Transfer the TR portion of Mreq and MAC1card,iss to the EFT terminal.

At the EFT terminal:

Step T5 When the Mreq is received at the terminal, the PAN field of Mreq is enciphered under the session key to meet any system privacy requirements. The enciphered PAN then replaces the clear PAN in the Mreq which may then be transmitted over the communication line to the acquirer for transmission to the issuer data processing centre via the packet switching system PSS (14 Fig. 1). The encipherment of PAN under the session key KS at the terminal may be performed by an Encipher Data (ECPH) operation defined by the following notation:

ECPH: $[E_{KMTi}KS,PAN] \rightarrow E_{KS}PAN.$

In executing this operation, a Decipher Key (DECK) operation is first performed to decipher $E_{KMTi}KS$ under the control of KMTi to obtain KS in clear form as the working key after which an Encipher (ENC) operation is performed to encipher PAN under control of KS to derive the enciphered PAN, i.e., $E_{KS}(PAN)$.

The Tterm,card field of Mreq is also enciphered in the same manner using the Encipher Data (ECPH) operation, as follows:

ECPH: $[E_{KMTi}KS, Tterm,card] \rightarrow E_{KS}Tterm,card$

and the enciphered Tterm,card replaces the clear Tterm,card in the Mreq.

Step T6 Transmit the received Mreq, MAC1card,iss, to the issuing agency data processing centre via the acquirer system and through a packet switched system node (14 Fig. 1).

At the Node (or Acquirer System):

Identify TID from received Mreq.

Step N1 Using a Translate Session Key (TRSK) operation, together with enciphered key parameters $E_{KM3acq}KNFacq$ and $E_{KM1acq}Klacq,sw$ obtained from the acquirer's cryptographic key data set (CKDS) and the stored enciphered session key $E_{KNFacq}KS$ for the terminal designated by TID, re-encipher KS from encipherment under the secondary file key KNFacq to encipherment under interchange key Klacq,sw (shared with the switch) to produce $E_{Klacq,sw}(KS)$, as follows:

TRSK: $[E_{KM3acq}KNFacq, E_{KNFacq}Ks, E_{KM1acq}Klacq,sw] \rightarrow E_{Klacq,sw}KS$

European Patent Application 821108/49 describes a system for performing the TRSK function.

Place $E_{Klacq,sw}KS$ in the transaction message request as shown in Fig. 13.

Step N2 Transmit Mreq to the PSS switch.

At the switch:

Step S1 Extract enciphered session key $E_{Klacq,sw}KS$ from Mreq. Using a Translate Session Key (TRSK) operation together with encphered key parameters $E_{KM3sw}Klacq,sw$ and $E_{KM1sw}Klsw,iss$ obtained from the switch's cryptographic key data set (CKDS) and the received enciphered session key $E_{Klacq,sw}KS$, re-encipher KS from encipherment under Klacq,sw to encipherment under Klsw,iss, as follows:

TRSK: $[E_{KM3sw}Klacq,sw, E_{Klacq,sw}KS, E_{KM1sw}Klsw,iss] \rightarrow E_{Klsw,iss}KS$

This re-enciphered session key, i.e., $E_{Klsw,iss}KS$, replaces the previously enciphered session key in Mreq which is then transmitted to the card issuing agency data processing centre.

Step S2 Transmit Mreq from the switch to the issuer.

At the Issuer DP Centre:

Step I1 Receive and store Mreq and index it using TID. Extract enciphered session key $E_{Klsw,iss}KS$ from Mreq. Using a Re-encipher to Master Key (RTMK) operation together with enciphered key parameter $E_{KM2iss}(Klsw,iss)$ obtained from the issuer's cryptographic key data set (CKDS) and the received enciphered session key $E_{Klsw,iss}KS$, re-encipher KS from encipherment under Klsw,iss to encipherment under the issuer's host master key (KM0iss), as follows:

RTMK: $[E_{KM2iss}Klsw,iss, E_{Klsw,iss}KS] \rightarrow E_{KM0iss}KS.$

Store $E_{KM0iss}KS$ and index using TID. Extract $E_{KS}Tterm,card$ from Mreq, and decipher the enciphered Tterm,card by a Decipher Data (DCPH) operation using the recovered enciphered session key $E_{KM0iss}KS$ to obtain Tterm,card in the clear as follows:

DCPH: [E_{KM0iss}KS, E_{KS}Tterm,card]→Tterm,card.

Replace the enciphered Tterm,card in Mreq with the clear Tterm,card.

Extract E_{KS}PAN from Mreq and store in temporary buffer. Using a Decipher Data (DCPH) operation together with the recovered enciphered session key E_{KM0iss}KS, decipher using KS to obtain PAN, as follows:

DCPH: [E_{KM0iss}KS, E_{KS}PAN]→PAN.

Step I2 The validity of PAN is checked by a table look-up process using the received deciphered PAN as an index to the table. If the PAN is valid then replace E_{KS}(PAN) with PAN in Mreq and continue at Step I3; otherwise continue at Step I17.

Step I3 Generate and store a pseudo-random or random time-variant quantity Tiss.

Step I4 Using an Encipher Master Key (EMK0) operation, encipher Tiss generated at Step I3 under the issuer's host master key (KM0iss), as follows:

EMK0: [Tiss]→E_{KM0iss}Tiss.

Generate and store the time-variant Tiss,term,card by using an Encipher Data (ECPH) operation together with the enciphered value of Tiss (i.e., E_{KM0iss}Tiss) used as a key to encipher Tterm,card received in Mreq to produce E_{Tiss}Tterm,card, as follows:

ECPH: [E_{KM0iss}Tiss,Tterm,card]→E_{Tiss}Tterm,card

where the desired Tiss,term,card is defined as quantity E_{Tiss}(Tterm,card).

Step I5 Generate KSTR2 using the RTMK operation of Fig. 3 together with the enciphered key parameter E_{KM2Iss}KNFiss obtained from the issuer's CKDS and Tiss,term,card obtained at Step I4 to produce E_{KM0iss}KSTR2, as follows:

RTMK: [E_{KM2Iss}(KNFiss), Tiss,term,card]→E_{KM0iss}(D_{KNFiss}Tiss,term,card)

where KSTR2 is defined as D_{KNFiss}Tiss,term,card.

Step I6 Generate KSTR1 using the RTMK operation of Fig. 3 together with the enciphered key parameter E_{KM2Iss}KTR1 for the particular cardholder with personal account number (PAN) obtained from the issuer's CKDS and Tterm,card received in Mreq to produce E_{KM0iss}KSTR1, as follows:

RTMK: [E_{KM2Iss}KTR1,Tterm,card]→E_{KM0iss}(D_{KTR1}Tterm,card)

where KSTR1 is defined as D_{KRT1}Tterm,card.

Step I7 Compute MAC1 card,iss of reference on the TR portion of the received Mreq by an Encipher Data (ECPH) operation (described by Fig. 7) using enciphered key parameter E_{KM0iss}KSTR1 (obtained at Step I6) as follows:

ECPH: [E_{KM0iss}KSTR1,TR]→MAC1card,iss

where the last or part of the last block of the resulting ciphertext is defined as MAC1card,iss of reference.

Step I8 If the MAC1card,iss of reference equals the received MAC1card,iss then accept the Mreq and continue at Step I9, otherwise reject Mreq and continue at Step I17.

Note that validating the MAC also simultaneously validates the received session key KS. If KS is changed, the deciphered value of Tterm,card would be in error and the MAC check in turn would fail.

A timeliness check at the issuer is, however, not possible since the issuer at this point has not received time-variant information it can check. (Note that Tterm,card as well as KS were generated outside the issuer and thus the timeliness of these values cannot be checked by the issuer). This does not present a security weakness because the information the issuer sends out at this point is of no value to an opponent. (Such information is obtainable by an opponent via stale messages sent to the issuer).

Step I9 If there is no reason to reject Mreq (e.g. funds are available, etc.), then continue at step I10 otherwise reject Mreq and continue at Step I17.

Step I10 Generate a first time variant authentication parameter (TAP1) using an RTMK operation together with the enciphered authentication parameter E_{KM2Iss}AP (for the particular cardholder with personal account number PAN) obtained from the issuer's CKDS and Tterm,card received in Mreq, as follows:

RTMK: [E_{KM2Iss}AP,Tterm,card]→E_{KM0Iss}(D_{AP} Tterm,card)=E_{KM0Iss}TAP1

where TAP1 is defined as D_{AP}(Tterm,card).

Also generate a second time variant authentication parameter (TAP2) using a DCPH operation together with the enciphered TAP1 (i.e., E_{KM0Iss}TAP1) used as a key parameter and Tiss,term,card obtained at Step I4 to obtain:

DCPH: [E_{KM0Iss}TAP1,Tiss,term,card]→D_{TAP1}Tiss,term,card

where TAP2 is defined as D_{TAP1}Tiss,term,card.

TAP1 is defined as D_{AP}Tterm,card and is obtained using the RTMK function of Fig. 6 where Q is AP (a quantity ($E_{KP⊕PIN}$PAN)⊕PAN pregenerated during the initialisation process) and KEY is Tterm,card. The result of the RTMK operation is E_{KM0}TAP1 as follow:

RTMK: [E_{KM2Iss}AP,Tterm,card]→E_{KM0}TAP1.

TAP2 is defined as D_{TAP1}Tiss,term,card and is obtained in a DCPH function by deciphering E_{KM0}TAP1 under the master key KM0 and then deciphering Tiss,term,card using TAP1 as the key as follows:

DCPH: [E_{KM0}TAP1,Tiss,term,card]→TAP2

In summary

AP=($E_{KP⊕PIN}$PAN)⊕PAN
TAP1=D_{AP}Tterm,card
TAP2=D_{TAP1}Tiss,term,card.

Thus, the correct generation TAP1 and TAP2 are directly dependent upon KP, PIN and PAN.

Step I11 Formulate Mresp as shown in Fig. 14.

Step I12 Compute MAC1iss,card on the card transaction response (CTR) portion of Mresp by an Encipher Data (ECPH) operation (described by Fig. 7) using enciphered key parameter E_{KM0}KSTR1 (obtained at Step I6) as follows:

ECPH: [E_{KM0Iss}KSTR1,CTR]→MAC1iss,card

where the last or part of the last block of resulting ciphertext is defined as MAC1iss,card. Transfer MAC1iss,card to Mresp.

Step I13 Compute MAC1iss,term on the terminal transaction response (TTR) portion of Mresp by an Encipher Data (ECPH) operation (described by Fig. 7) using enciphered key parameter E_{KM0Iss}KSTR2 (obtained at Step I5) as follows:

ECPH: [E_{KM0Iss}KSTR2,TTR]→MAC1iss,term

where the last or part of the last block of resulting ciphertext is defined as MAC1iss,term. Transfer MAC1iss,term to Mresp.

Step I14 Re-encipher the transmission session key KSTR2 from encipherment under the issuer's host master key (KM0iss), i.e., E_{KM0Iss}KSTR2, to encipherment under the interchange key Kliss,sw, i.e., $E_{Kliss,sw}$KSTR2 by a Re-encipher From Master Key (RFMK) operation using the enciphered key parameter E_{KM1Iss}Kliss,sw obtained from the issuer's CKDS and the stored enciphered transaction key, i.e., E_{KM0Iss}KSTR2 as follows:

RFMK: [E_{KM1Iss}Kliss,sw, E_{KM0Iss}KSTR2]→$E_{Kliss,sw}$KSTR2.

Transfer $E_{Kliss,sw}$KSTR2 to Mresp.

Step I15 Transfer E_{KS}PAN from buffer (Step I1) to Mresp. Where KP is less than a predetermined number of bits then TAP2 is also enciphered under KS using an ECPH function as follows:

ECPH: [E_{KM0Iss}KS, TAP2]→E_{KS}TAP2.

Transfer TAP2 or the enciphered TAP2 to Mresp depending on the size of KP.

Step I16 Send Mresp to the PSS network. Continue at Step S3.

Step I17 Negative response routine. Formulate Mresp as shown in Fig. 15. The data field will include information on why the transaction is not to be honoured, i.e., lack of funds, MAC check failure, etc. The message will also include Tiss.

Step I18 Compute MAC1iss,term on the TTR portion of the negative Mresp by an Encipher Data (ECPH) operation (described by Fig. 7) using enciphered key parameter E_{KM0iss}KSTR2 (obtained at Step I5) as follows:

ECPH: [E_{KM0iss}KSTR2,TTRD]→MAC1iss,term

where the last or part of the last block of resulting ciphertext is defined as MAC1iss,term.
Transfer MAC1iss,term to Mresp.

Step I19 Send Mresp to the PSS network. Continue at S3.

At the PSS Switch:

Step S3 Extract enciphered session key $E_{Klsw,iss}$KSTR2 from Mresp. Using a Translate Session Key (TRSK) operation together with enciphered key parameters E_{KM3sw}Kliss,sw and E_{KM1sw}Klsw,acq obtained from the switch's CKDS and the received enciphered session key $E_{Kliss,sw}$KSTR2, reencipher KSTR2 from encipherment under Kliss,sw to encipherment under Klsw,acq, as follows:

TRSK: [E_{KM3sw}Kliss,sw, $E_{Kliss,sw}$KSTR2, E_{KM1sw}Klsw,acq]
→$E_{Klsw,acq}$KSTR2

Step S4 Replace $E_{Kliss,sw}$KSTR2 with $E_{Klsw,aq}$KSTR2 in Mresp.

Step S5 Send positive or negative Mresp to the acquirer as appropriate.

At the Acquirer:

Step N3 Extract enciphered transaction session key $E_{Klsw,acq}$KSTR2 from Mresp. Using a Translate Session Key (TRSK) operation together with enciphered key parameters E_{KM3acq}Klsw,acq and E_{KM1acq}KMT obtained from the acquirer's CKDS, re-encipher KSTR2 from encipherment under Klsw,acq to encipherment under KMT (for the terminal with terminal identifier TID), to produce E_{KMT}KSTR2 as follows:

TRSK: [E_{KM3acq}Klsw,acq, $E_{Klsw,acq}$KSTR2, E_{KM1acq}KMT]→E_{KMT}KSTR2

Step N4 Replace $E_{Klsw,acq}$KSTR2 with E_{KMT}KSTR2 in Mresp.

Step N5 Send positive or negative Mresp to the terminal as appropriate.

At the EFT terminal

Step T7 Check to determine whether the message has been received within a predetermined time period by using a time-out procedure. If the time is not exceeded then proceed to Step T8, else continue at Step T22.

Step T8 Decipher the enciphered PAN, i.e., E_{KS}PAN, by a Decipher Data (DCPH) operation the previously stored enciphered session key E_{KMT}KS and E_{KS}PAN received in Mresp as follows:

DCPH: [E_{KMT}KS, E_{KS}PAN]→PAN

Store E_{KS}PAN in a temporary buffer and replace E_{KS}PAN with the deciphered PAN in Mresp.
If TAP2 is in enciphered form, i.e., E_{KS}TAP2, then decipher E_{KS}TAP2 by a Decipher Data (DCPH) operation using the previously stored E_{KMT}KS and E_{KS}(TAP2) received in Mresp as follows:

DCPH: [E_{KMT}KS, E_{KS}TAP2]→TAP2

Step T9 Store E_{KMT}KSTR2 in an appropriate buffer.

Step T10 If Mresp is non-negative then go to step T11; otherwise, if negative go to Step T14.

Step T11 Compute MAC1iss,term of reference on the TTR portion of the received Mresp by an Encipher Data (ECPH) operation (described by Fig. 7) using received enciphered key parameter E_{KMT}KSTR2 (obtained from Mresp at Step T9) as follows:

ECPH: [E_{KMT}KSTR2,TTR]→MAC1iss,term

where the last or part of the last block of resulting ciphertext is defined as MAC1iss,term of reference. If MAC1iss,term of reference equals received MAC1iss,term, then accept received message and go to Step T12; otherwise, go to Step T14.

Step T12 If received Tterm,card equals stored Tterm,card (Step T1), then continue at Step T13; otherwise go to Step T14.

Step T13 Send the CTR and MAC1iss,card portions of Mresp to the personal portable microprocessor (ppm). Go to Step C7.

Step T14 For a negative response message, computer MAC1iss,term of reference on the TTRD portion of the received negative Mresp by an Encipher Data (ECPH) operation (described by Fig. 7) using received enciphered key parameter E_{KMT}KSTR2 (obtained from Mresp in Step T9) as follows:

ECPH: [E_{KMT}KSTR2, TTRD]→MAC1iss,term

where the last or part of the last block of resulting ciphertext is defined as MAC1iss,term of reference. If MAC1iss,term of reference equals received MAC1iss,term then continue at Step T15, else go to Step 16.

Step T15 If received Tterm,card equals stored Tterm,card (Step T1) then abort the transaction and continue at Step T22. (Since a definite negative replay has been received from the issuer, no retry is allowed). Otherwise, go to Step 16.

Step T16 The timeliness check and/or MAC check failed.

Since there is a doubt on the negative or non-negative response the system rules may allow one or more retry. That is a return to Step C1. After a limited number of unsuccessful retries, abort transaction and continue at Step T22.

At the ppm:

Step C7 Receive the CTR and MAC1iss,card portions of Mresp and store Tiss.

Step C8 Computer MAC1iss,card of reference on the CTR portion of the received Mresp using stored key parameter KSTR1 (Step C4) as the enciphering key. Generation of a message authentication code is illustrated in Fig. 7.

Step C9 If MAC1iss,card of reference equals received MAC1iss,card then accept Mresp and continue at Step C10; otherwise continue at Step C17.

Step C10 If received Tterm,card equals stored Tterm,card (Step C4) then accept Mresp and continue at Step H1; otherwise, continue at Step C17.

At this point the EFT terminal will display a message indicating to the user that the cardholder is now required to enter the PIN on the terminal consumer module (28 Fig. 2) if there is agreement on transaction details, amount, etc.

At User Cardholder:

Step H1 Enter PIN into card via terminal after agreeing to the transaction details (e.g., amount, etc.). Then continue at Step C11.

At the ppm:

Step C11 Compute TAP1 using PAN, KP, PIN and stored Tterm,card.

The card user's identification PAN is enciphered using an XOR function of KP and the entered PIN as a key. The result of the first encipher operation is XOR'd with PAN defining AP. The stored Tterm,card is then deciphered using AP as the key to produce TAP1.

Step C12 Generate KSTR3 using PAN, KP, PIN and stored PIN and Tiss,term,card.

The generation of KSTR3 is illustrated in Fig. 8. The card users identification PAN is deciphered using an XOR function on PIN and KP as the key. The result of the first decipher operation is XOR'd with PAN defining KTR2. Tiss,card,term is then deciphered using KTR2 as the key to produce the transaction session key KSTR3.

Step C13 Store KSTR3 and destroy PIN value.

Step C14 Send TAP1 to terminal.

At the EFT Terminal:

Step T17 Compute Tiss,term,card from stored Tterm,card and issuer received Tiss. Compute TAP2 from Card-received TAP1 and Tiss,term,card.

The computation of Tiss,term,card is illustrated in Fig. 9. Tiss received in Mresp is first loaded as a working key using a Load Key Direct (LKD) operation. The stored value of Tterm,card is enciphered under Tiss using an Encipher (ENC) operation to produce E_{Tiss}Tterm,card, as follows:

LKD: [Tiss]

ENC: [Tterm,card]→E_{Tiss}Tterm,card.

The computation of TAP2 is accomplished as follows. The card-received TAP1 is first loaded as a

working key using a Load Key Direct (LKD) operation. The generated value of Tiss,term,card is deciphered under TAP1 using a Decipher (DEC) operation to produce D_{TAP1}Tiss,term,card, as follows:

LKD: [TAP1]
DEC: [Tiss,term,card]→D_{TAP1}Tiss,term,card

where TAP2 is defined equal to D_{TAP1}Tiss,term,card.

Step T18 If TAP2 equals received TAP2 of reference, then accept PIN and continue at Step T19; otherwise if re-entry of the PIN is permitted, as the predetermined number of failed attempts is *not exhausted* THEN continue at Step H1; ELSE continue at Step T22.
Step T19 Complete the card holder transaction (i.e., hand over goods, print receipt, etc.).
Step T20 If completion successful THEN continue at Step T21; ELSE continue at Step T22.
Step T21 Formulate Message status Mstat (reflecting the outcome of the transaction) and send the CSD portion of Mstat to ppm. Continue at C15. The format of the Mstat is shown in Fig. 16.
Step T22 A negative condition has been detected by the terminal (e.g., response timeout, MAC1iss,term check failed, a negative Mresp from issuer due to MAC1card,iss check failure at issuer, printer failure, PIN invalid, etc.).
Step T23 Formulate a negative status message Mstat as shown in Fig. 17 and continue at Step T24. (The code word portion of Mstat indicates whether Mstat represents a positive or negative status message).
Step T24 Store E_{KS}(PAN) from the Mresp. Compute MAC2term,iss on the TSD portion of Mstat (Fig. 16) or on the TFD portion of the negative Mstat (Fig. 17), as appropriate, by an Encipher Data (ECPH) operation (described by Fig. 7) using enciphered key parameter E_{KMT}KSTR2 (obtained from Mresp in Step T9) as follows:

ECPH: [E_{KMT}KSTR2,TSD]→MAC2term,iss

or

ECPH: [E_{KMT}KSTR2,TFD]→MAC2term,iss

where the last or part of the last block of resulting ciphertext is defined as MAC2term,iss.
Replace clear PAN with E_{KS}PAN. Encipher the received TAP1 (Step T17) by an Encipher Data (ECPH) operation using previously stored enciphered session key E_{KMT}KS as follows:

ECPH: [E_{KMT}KS, TAP1]→E_{KS}TAP1

Replace TAP1 with E_{KS}TAP1 in Mstat.
Step T25 Send Mstat to issuer via acquirer and switch (MAC2card,iss will be absent in all negative status conditions). Conclude processing at the terminal and continue at Step I20.

If a Mstat is generated because a MAC check has failed on either a positive or negative Mresp, then a Network Administration Centre processor is informed so that system failures can be monitored and possible faults corrected.

At the ppm:
Step C15 Receive CSD portion of Mstat from terminal. Compute MAC2card,iss on the CSD portion of Msfat using stored key parameter KSTR3 (Step C13) as the enciphering key. Generation of a message authentication code is illustrated in Fig. 7.
Step C16 Send positive response and MAC2card,iss to terminal and continue at Step T24.
Step C17 Send negative response to terminal indicating that MAC check at Step C9 has failed, and continue at Step T23. (A MAC is not calculated here because the check for MAC1iss,card which is end-to-end, failed. Most likely another end-to-end MAC will not be successful either).

At the Issuer Host:
Step I20 Receive Mstat. If a Positive Mstat is received continue at Step I21; otherwise, if a negative Mstat is received continue at Step I31.
Step I21 Process positive Mstat. Extract E_{KS}TAP1 as appropriate and E_{KS}PAN from positive Mstat and decipher the enciphered TAP1 (as appropriate) and PAN, i.e., E_{KS}TAP1 and E_{KS}PAN, by a Decipher Data (DCPH) operation using the previously stored enciphered session key E_{KM0Iss}KS (Step I1) as follows:

DCPH: [E_{KM0Iss}KS, E_{KS}TAP1]→TAP1

DCPH: [E_{KM0Iss}KS, E_{KS}PAN]→PAN.

Replace enciphered TAP1 (as appropriate) and PAN with clear TAP1 and PAN in Mstat.

Step I22 Extract Tiss from Mstat and encipher Tiss under the issuer's host master key (KM0iss) by an Encipher Master Key (EMKØ) operation as follows:

EMKØ: [Tiss]→E_{KM0iss}Tiss.

Extract Tterm,card from Mstat, and generate the time-variant Tiss,term,card by an Encipher Data (ECPH) operation using enciphered Tiss, i.e., E_{KM0iss}Tiss, as the key, as follows:

ECPH: [E_{KM0iss}Tiss,Tterm,card]→E_{Tiss}Tterm,card

where Tiss,term,card is defined as E_{Tiss}Tterm,card.

Step I23 Regenerate KSTR2 by an RTMK operation using enciphered key parameter E_{KM2iss}KNFiss obtained from the issuer's CKDS and Tiss,term,card obtained at Step I22 to produce E_{KM0iss}KSTR2, as follows:

RTMK: [E_{KM2iss}KNFiss,Tiss,term,card]→
$E_{KM0iss}D_{KNFiss}$Tiss,term,card

where KSTR2 is defined as D_{KNFiss}Tiss,term,card.

Step I24 Compute MAC2term,iss of reference on the TSD portion of the received Mstat by an Encipher Data (ECPH) operation (described by Fig. 7) using enciphered key parameter E_{KM0iss}KSTR2 (regenerated at Step I23) as follows:

ECPH: [E_{KM0iss}KSTR2,TSD]→MAC2term,iss

where the last or part of the last block of resulting ciphertext is defined as MAC2term,iss of reference. If computed MAC2term,iss of reference equals MAC2term,iss received in Mstat, then continue at Step I25; otherwise continue at Step I30.

Step I25 If computed Tiss,term,card (Step I22) equals stored Tiss,term,card (Step I4), then continue at Step I26; otherwise, continue at Step I30.

Step I26 Generate KSTR3 by an RTMK operation (Fig. 8) using enciphered key parameter E_{KM2iss}KTR2, obtained from the issuer's CKDS for the particular cardholder with personal account number (PAN), and Tiss,term,card generated at Step I23, to produce E_{KM0iss}(KSTR3), as follows:

RTMK: [E_{KM2iss}KTR2, Tiss,term,card]→$E_{KM0iss}D_{KTR2}$Tiss,term,card

where KSTR3 is defined as D_{KTR2}Tiss,term,card.

Step I27 Compute MAC2card,iss of reference on the CSD portion of the received Mstat by an Encipher Data (ECPH) operation (described by Fig. 7) using enciphered key parameter E_{KM0iss}KSTR3 (generated at Step I26) as follows:

ECPH: [E_{KM0iss}KSTR3,CSD]→MAC2card,iss

where the last or part of the last block of resulting ciphertext is defined as MAC2card,iss of reference. If computed MAC2card,iss of reference equals MAC2card,iss received in Mstat, then continue at Step I28; otherwise, continue at Step I30.

Step I28 Accept the transaction and update records.

Step I29 Formulate a positive acknowledgement message (Mack) and send Mack to the acquirer system or to the terminal's sponsor host. Continue at Step I37.

Step I30 Reject the transaction and initiate a negative acknowledgement message (Mnak) and send Mnak to the terminal and the Network Administration Centre.

Step I31 Process negative Mstat. generate KSTR2 by an RTMK operation using enciphered key parameter E_{KM2iss}KNFiss obtained from the issuer's CKDS and stored Tiss,term,card obtained at Step I4 to produce E_{KM0iss}KSTR2, as follows:

RTMK: [E_{KM2iss}KNFiss, Tiss,term,card]→$E_{KM0iss}D_{KNFiss}$Tiss,term,card

where KSTR2 is defined as D_{KNFiss}Tiss,term,card.

Step I32 Compute MAC2term,iss of reference on the TFD portion of the received Mstat by an Encipher Data (ECPH) operation (described by Fig. 7) using enciphered key parameter E_{KM0iss}KSTR2 (regenerated at Step I31) as follows:

ECPH: [E_{KM0iss}KSTR2, TFD]→MAC2term,iss

where the last or part of the last block of resulting ciphertext is defined as MAC2term,iss of reference. If computed MAC2term,iss of reference equals MAC2term,iss received in the negative Mstat, then continue at Step I33; otherwise continue at Step I36.

Step I33 Extract Tiss from the received negative Mstat. If the received Tiss equals stored Tiss (Step I3), then continue at Step I34; otherwise, continue at Step I36.

Step I34 Accept the negative Mstat and update records.

Step I35 Formulate a positive acknowledgement message (Mack) and send Mack to the acquirer system or to the terminal's sponsor host. Continue Step I37.

Step I36 Reject the negative Mstat and initiate a negative acknowledgement message (Mnak) and send Mnak to the terminal and the Network Administration Centre.

Step I37 Halt procedure.

Figures 10, 11 and 12 illustrate the sequence of the steps of the method in a flow chart form. Starting with Step C1 at the personal portable microprocessor (Fig. 10) the steps continue to I37 (Fig. 12) which ends the transaction.

The system described above has the added advantage in that when the POS terminal is in a supermarket environment the personal verification check which typically should take between 1—5 seconds can be initiated before the goods are totalled and completed well before the total amount due has been calculated. Unless there is some valid reason for referring the user's card there should be no additional delay at the terminal for customers using the EFT system for payment of goods.

Claims

1. An electronic funds transfer system in which EFT terminals are connected through a local data processing centre (acquirer) to a public switch system (switch), a plurality of card-issuing agencies' data processing centres are also connected to the public switch system and each user of the EFT system has a personal secure intelligent bank card on which is stored a personal account number (PAN) and a personal key (KP), the system including

means at each local data processing centre to generate session keys (KS) for each of its locally attached terminals, and to transmit an associated session key to a respective terminal,

at each terminal means to store the session key,

means to encipher sensitive data (PAN) under the session key whenever a transaction request message is generated,

means to generate a transaction variable for each transaction initiated at the terminal and to transfer the transaction variable to the card;

means to transfer a message request including the transaction variable enciphered under KS to the users card and means on the card to generate a message authentication code using a time-variant key (KSTR1) based upon the users PAN, KP and the transaction variable,

means at each local data processing centre to encipher the appropriate session key under a cross-domain key whenever a transaction request message is received and to add the enciphered key to the message,

means at each processing node of the public switch system to translate the enciphered session key from encipherment under a received cross-domain key to a transmission cross-domain key,

means at the card issuing agency's data processing centre to decipher the enciphered session key and to use the key to decipher any sensitive data contained in the request message, and

means to regenerate the message authentication code using the time variant key (KSTR1) which is generated from parameters based upon the PAN and KP and the received transaction variable for comparison with the message authentication code included in the received message.

2. An electronic funds transfer system as claimed in Claim 1 further including

means at the card and terminal for each transaction initiated at the terminal to generate a first transaction variable (Tterm,card) and to include the first transaction variable in a transaction message request sent to the c.i.a. data processing centre (steps C1—T6 (Fig. 10)),

the system also including at the c.i.a. data processing centres,

means to construct a response message to each transaction request message received, each positive response message including a first portion (CTR) on which a first message authentication code is generated using a key derived from the first transaction variable, the user's personal key and personal account number, and a second portion including the first portion on which a second message authentication code is generated using as an encipher key a random or pseudo-random number and means to encipher the random number key under a cross-domain key and to add the enciphered key to response message (steps I1—I19 (Fig. 10)),

means at the terminal to receive the response message and to decipher the random number key, to use the deciphered key to recreate a message authentication code based upon the second portion of the received message and to compare the recreated message authentication code with the received second message authentication code (steps T7—T13 (Fig. 11)),

means at the card to use the first transaction variable, the personal key and the personal account

number to derive an encipher key to generate a message authentication code on the first portion of the message and to compare the recreated message authentication code with the received first message authentication code (steps C7—C14 (Fig. 11)).

Patentansprüche

1. Elektronisches Geldüberweisungssystem (EFT), in welchem EFT-Benutzerstationen über ein lokales Datenverarbeitungszentrum (Erwerber) an ein öffentliches Schaltsystem (Schalter) angeschlossen sind, eine Vielzahl an Datenverarbeitungszentren von kartenausgebenden Verkaufspunkten ebenfalls an das öffentliche Schaltsystem angeschlossen sind und jeder Benutzer des EFT-Systems eine gesicherte persönliche intelligente Bankkarte besitzt, auf welcher eine persönliche Kontonummer (PAN) und ein persönlicher Schlüssel (KP) gespeichert sind, wobei das System aufweist:

an jedem lokalen Datenverarbeitungszentrum Einrichtungen, um Sitzungsschlüssel (KS) für jeden seiner lokal angeschlossenen Benutzerstationen zu generieren und um einen zugehörigen Sitzungsschlüssel an eine zugehörige Benutzerstation zu übertragen,

an jeder Benutzerstation Einrichtungen um den Sitzungsschlüssel zu speichern,

Einrichtungen aufweist, um jedesmal, wenn eine Anforderungsmeldung für eine Transaktion generiert wird, vertrauliche Daten (PAN) nach dem Sitzungsschlüssel zu verschlüsseln,

Einrichtungen, um eine Transaktionsvariable für jede Transaktion, die an der Benutzerstation begonnen wird, zu generieren und um diese Transaktionsvariable auf die Kart zu übertragen,

Einrichtungen, um eine Anforderungsmeldung, einschließlich der Transaktionsvariablen, welche nach KS verschlüsselt ist, auf die Benutzerkarte zu übertragen, und Einrichtungen auf der Karte, um einen Berechtigungscode für Meldungen zu generieren, unter Verwendung eines zeitlich-variablen Schlüssels (KSTR1), welcher auf den PAN und KP des Benutzers und der Transaktionsvariable basiert,

an jedem lokalen Datenverarbeitungszentrum Einrichtungen, um den geeigneten Sitzungsschlüssel nach einem Mehrdomänenschlüssel zu verschlüsseln, jedesmal wenn eine Anforderungsmeldung für eine Transaktion empfangen wird und, um den verschlüsselten Schlüssel zu der Meldung zu fügen,

Einrichtungen an jedem Verarbeitungsknoten des öffentlichen Schaltsystems, um den verschlüsselten Sitzungsschlüssel von der Verschlüsselung nach einem empfangenen Mehrdomänenschlüssel in einen Übertragungs-Mehrdomänenschlüssel zu übersetzen,

Einrichtungen an dem Datenverarbeitungszentrum des kartenausgebenden Verkaufspunkts, um den verschlüsselten Sitzungsschlüssel zu entschlüsseln und um den Schlüssel zur Entschlüsselung jeglicher vertraulicher Daten, welche in der Anforderungsmeldung enthalten sind, zu verwenden, und

Einrinchtungen, um den Berechtigungscode für Meldungen zu regenerieren, unter Verwendung des zeitlich-variablen Schlüssels (KSTR1), welcher aus Parametern generiert wird, die auf den PAN, KP und der empfangenen Transaktionsvariable basieren, für den Vergleich mit dem in der empfangenen Meldung enthaltenen Berechtigungscode für Meldungen.

2. Elektronisches Geldüberweisungssystem nach Anspruch 1, welches weiters

Einrichtungen auf der Karte und an der Benutzerstation aufweist, welche für jede Transaktion, die an der Benutzerstation begonnen wird, eine erste Transaktionsvariable (Tterm,card) generieren und die erste Transaktionsvariable in eine Anforderungsmeldung für eine Transaktion einschließen, welche dem c.i.a. Datenverarbeitungszentrum gesendet wird (Schritte C1—T6 (Fig. 10)),

wobei das System an den c.i.a. Datenverarbeitungszentren

Einrichtungen aufweist, um eine Antwortmeldung auf jede Anforderungsmeldung für eine Transaktion zu erstellen, wobei jede positive Antwortmeldung einen ersten Teil (CTR) aufweist, mittels dem unter Verwendung eines von der ersten Transaktionsvariable, dem persönlichen Schlüssel und der persönlichen Kontonummer des Benutzers abgeleiteten Schlüssels ein erster Berechtigungscode für Meldungen generiert wird, und einen zweiten Teil, der den ersten Teil beinhaltet, mittels dem ein zweiter Echtheitscode für Meldungen generiert wird, wobei als Verschlüsselungsschlüssel eine Zufalls- oder Pseudozufallszahl verwendet wird, und (weiters) Einrichtungen, um den Zufallszahlenschlüssel nach einem Mehrdomänenschlüssel zu verschlüsseln und um den verschlüsselten Schlüssel zu der Antwortmeldung zu fügen (Schritte I1—I19 (Fig. 10)),

an der Benutzerstation Einrichtungen aufweist, die die Antwortmeldung empfangen und den Zufallszahlenschlüssel entschlüsseln, die den entschlüsselten Schlüssel verwenden, um einen Berechtigungscode für Meldungen neu zu erstellen, welcher auf dem zweiten Teil der empfangenen Meldung basiert, und die den neuerstellten Berechtigungscode für Meldungen mit dem empfangenen zweiten Berechtigungscode für Meldungen vergleichen (Schritte T7—T10 (Fig. 11)) und

Einrichtungen auf der Karte aufweist, die die erste Transaktionsvariable, den persönlichen Schlüssel und die persönliche Kontonummer verwenden, um einen Verschlüsselungsschlüssel abzuleiten, der einen Berechtigungscode für Meldungen mittels des ersten Teils der Meldung generiert, und die den neuerstellten Berechtigungscode für Meldungen mit dem empfangenen ersten Berechtigungscode für Meldungen vergleichen (Schritte C7—C14 (Fig. 11)).

Revendications

1. Système électronique de transfert de fonds dans lequel des terminaux EFT sont connectés par

l'intermédiaire d'un centre local de traitement de données (unité de saisie) à un système de commutation public (commutateur), une pluralité de centres de traitement de données d'organisations d'émission de cartes sont également connectés au système de commutation public, et chaque utilisateur du système EFT possède une carte bancaire intelligente personnelle de sécurité sur laquelle sont stockés un numéro de compte personnel (PAN) et une clé personnelle (KP), le système comprenant

des moyens, à chaque centre local de traitement de données, pour générer des clés de session (KS) pour chacun de ses terminaux localement raccordés, et pour transmettre une clé de session associée à un terminal respectif,

à chaque terminal, des moyens pour stocker la clé de session,

des moyens pour chiffrer les données confidentielles (PAN) selon la clé de session, chaque fois qu'un message de demande de transaction est généré,

des moyens pour générer une variable de transaction pour chaque transaction commencée au terminal et pour transférer la variable de transaction à la carte,

des moyens pour transférer un message de demande comprenant la variable de transaction chiffrée selon KS à la carte d'utilisateur, et des moyens prévus sur la carte pour générer un code d'authentification de message en utilisant une clé variant dans le temps (KSTR1) basée sur les PAN et KP d'utilisateur et sur la variable de transaction,

des moyens, à chaque centre local de traitement de données, pour chiffrer la clé de session appropriée selon une clé inter-domaine chaque fois qu'un message de demande de transaction est reçu et pour ajouter la clé chiffrée au message,

des moyens, à chaque noeud de traitement du système de commutation public, pour traduire la clé de session chiffrée du chiffrement selon une clé interdomaine reçue à une clé inter-domaine de transmission,

des moyens, au centre de traitement de données de l'organisation d'émission de cartes, pour déchiffrer la clé de session chiffrée et pour utiliser la clé au déchiffrement de toutes données confidentielles contenues dans le message de demande, et

des moyens pour recréer le code d'authentification de massage au moyen de la quantité à variance de temps (KSTR1) qui est générée à partir de paramètres basés sur les PAN et KP et sur la variable de transaction reçue, pour comparaison avec le code d'authentification de message inclus dans le message reçue.

2. Système électronique de transfert de fonds suivant la revendication 1, comprenant en outre

des moyens, sur la carte et au terminal, pour chaque transaction commencée au terminal, pour générer une première variable de transaction (Tterm,card) et pour inclure la première variable de transaction dans un message de demande de transaction envoyé au centre de traitement de données de l'organisation d'émission de cartes (Etapes C1—T6 (Figure 10)),

le système comprenant également, aux centres de traitement de données d'organisation d'émission de cartes,

des moyens pour construire un message de réponse à chaque message de demande de transaction reçu, chaque message de réponse positif comportant une première partie (CTR) sur laquelle un premier code d'authentification de message est généré au moyen d'une clé obtenue à partir de la première variable de transaction, de la clé personnelle et du numéro de compte personnel de l'utilisateur, et une deuxième partie comprenant la première partie sur laquelle un deuxième code d'authentification de message est généré en utilisant comme clé de chiffrement un nombre aléatoire ou pseudo-aléatoire, et des moyens pour chiffrer la clé de nombre aléatoire selon une clé inter-domaine et pour ajouter la clé chiffrée au message de réponse (Etapes I1—I19 (figure 10)),

des moyens, au terminal, pour recevoir le message de réponse et déchiffrer la clé de nombre aléatoire, pour utiliser la clé déchiffrée afin de recréer un code d'authentification de message sur la base de la deuxième partie du message reçu, et pour comparer le code d'authentification de message recréé avec le deuxième code d'authentification de message reçu (Etapes T7—T13 (figure 11)),

des moyens, sur la carte pour utiliser la première variable de transaction, la clé personnelle et le numéro de compte personnel de manière à obtenir une clé de chiffrement pour générer un code d'authentification de message sur la première partie du message, et pour comparer le code d'authentification de message recréé avec le premier code d'authentification de message reçu (Etapes C7—C14 (figure 11)).

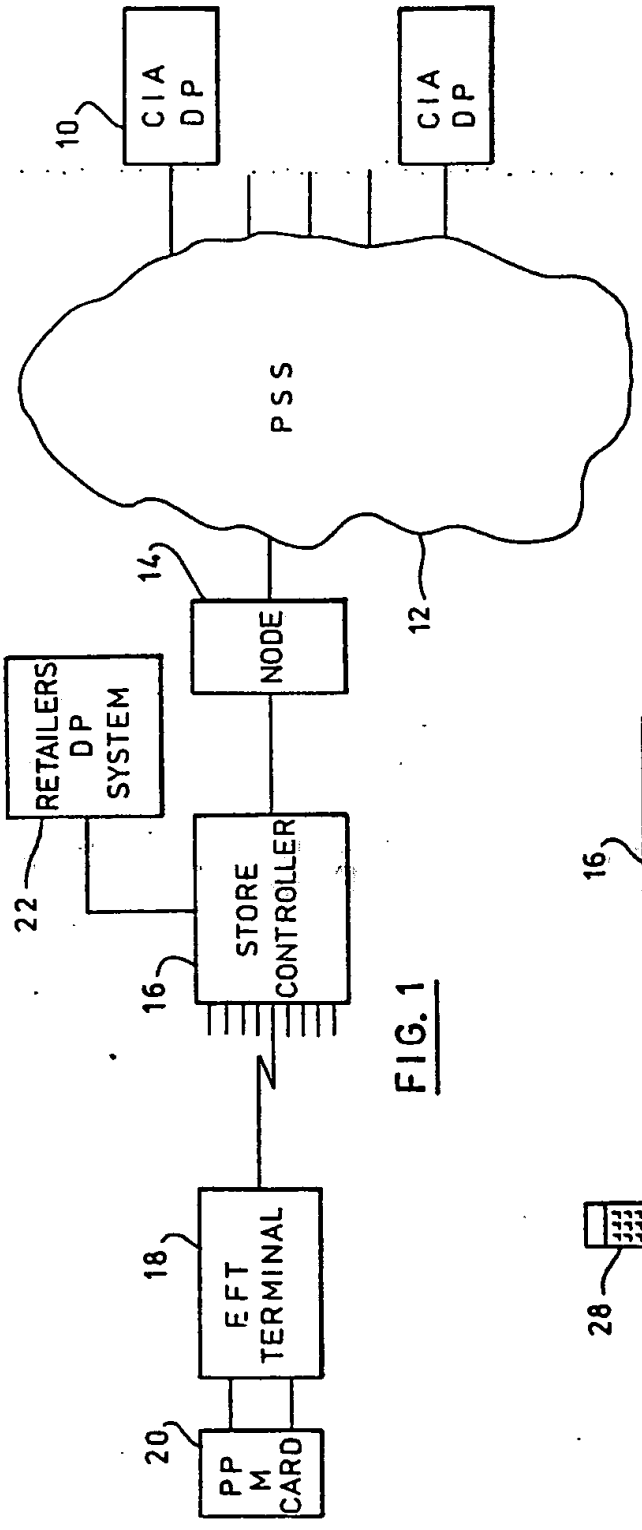

CIA DP
CIA DP
10
PSS
12
14
NODE
RETAILERS DP SYSTEM
22
STORE CONTROLLER
16
18
EFT TERMINAL
20
PP M CARD

FIG. 1

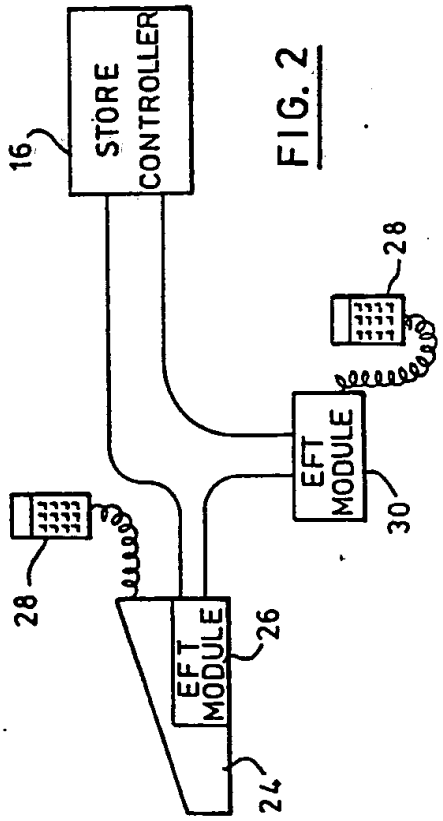

16
STORE CONTROLLER
28
28
EFT MODULE
30
EFT MODULE
26
24

FIG. 2

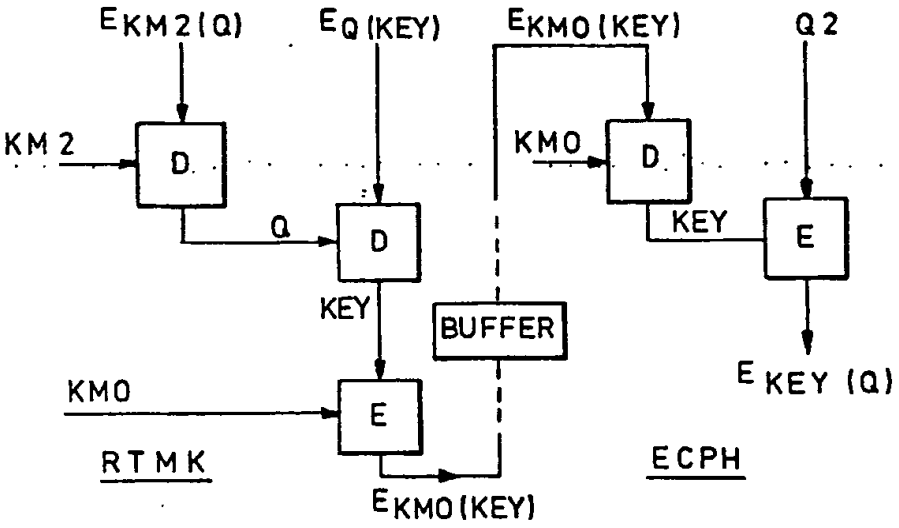

EKM2(Q)
EQ(KEY)
EKMO(KEY)
Q2
KM2
D
KMO
D
Q
D
KEY
E
KEY
BUFFER
EKEY(Q)
KMO
E
RTMK
ECPH
EKMO(KEY)

FIG. 3

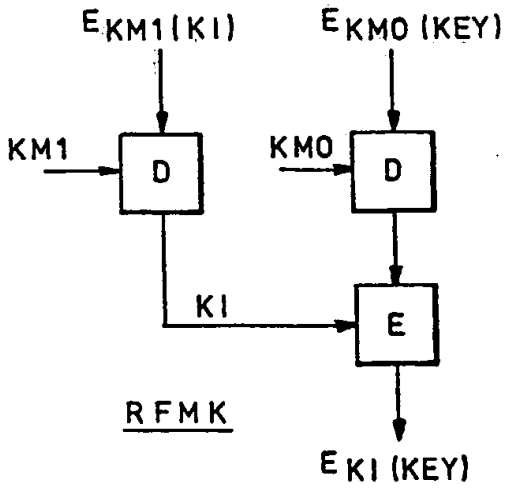

EKM1(KI)
EKMO(KEY)
KM1
D
KMO
D
KI
E
RFMK
EKI(KEY)

FIG. 4

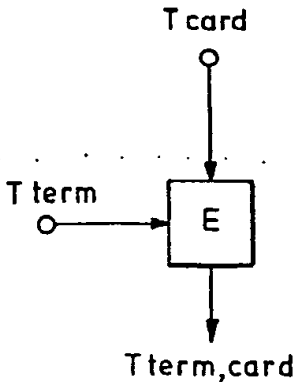


FIG. 5

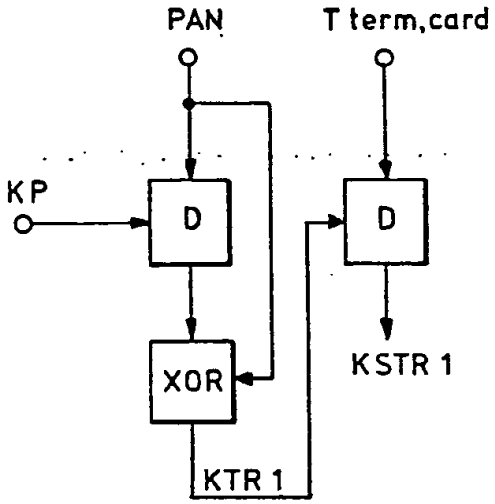


FIG. 6

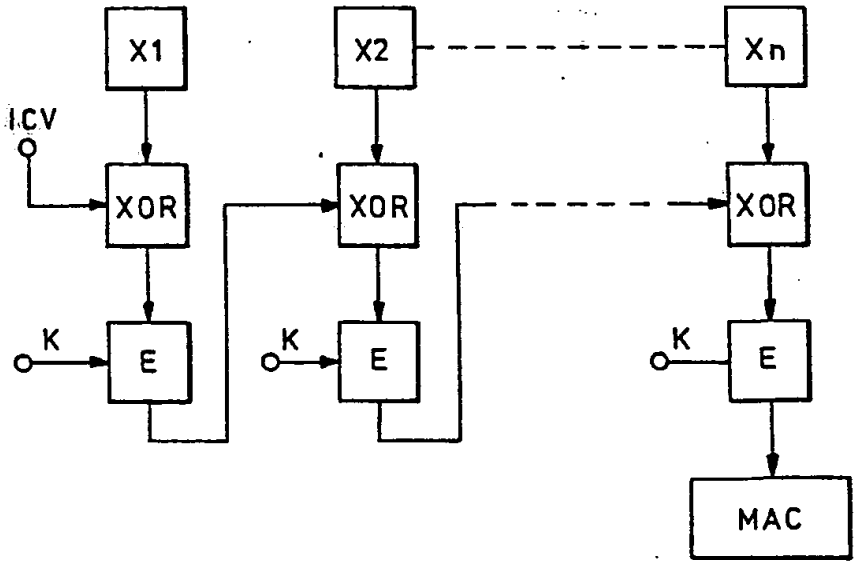


FIG. 7

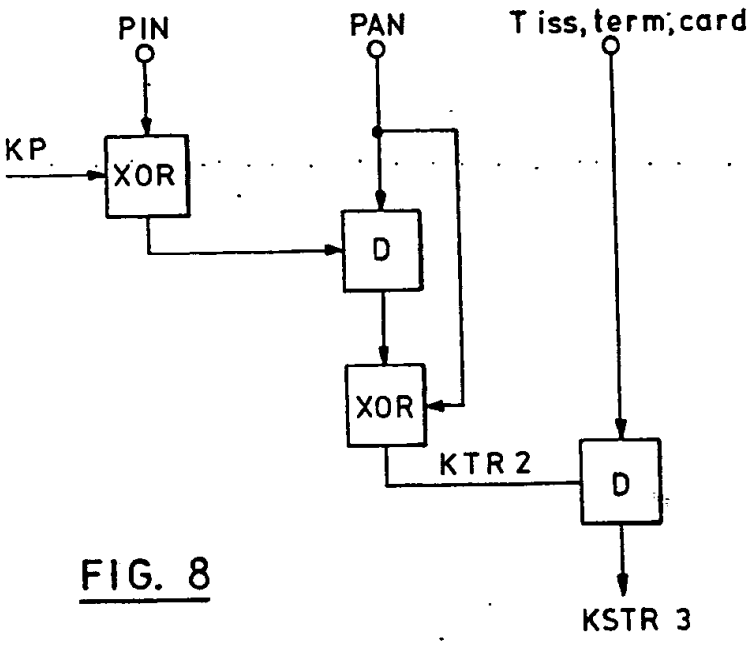

PIN
PAN
T iss, term, card
KP
XOR
D
XOR
KTR 2
D
KSTR 3

FIG. 8

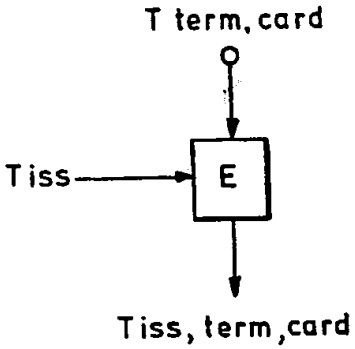

T term, card
Tiss
E
Tiss, term, card

FIG. 9

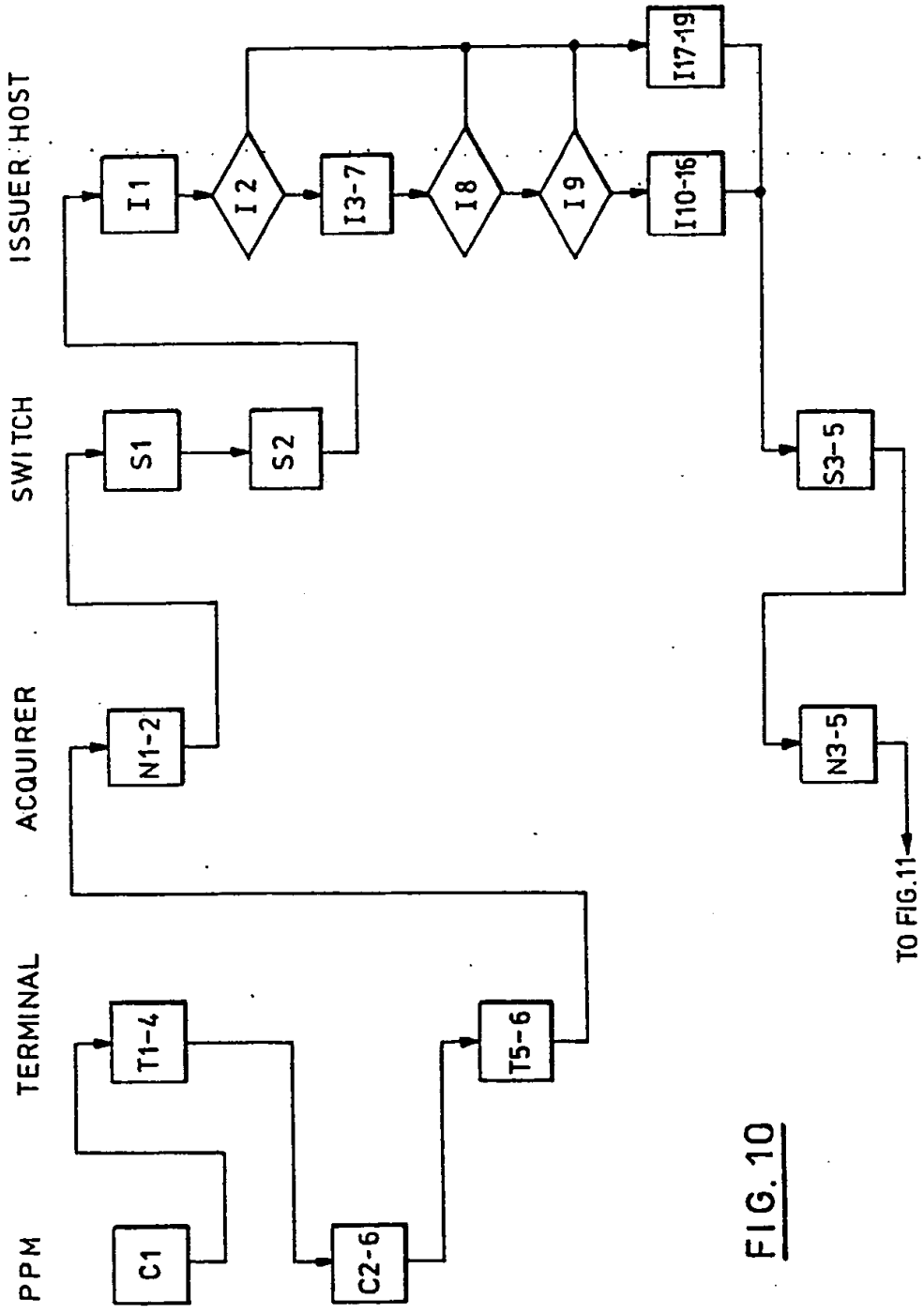
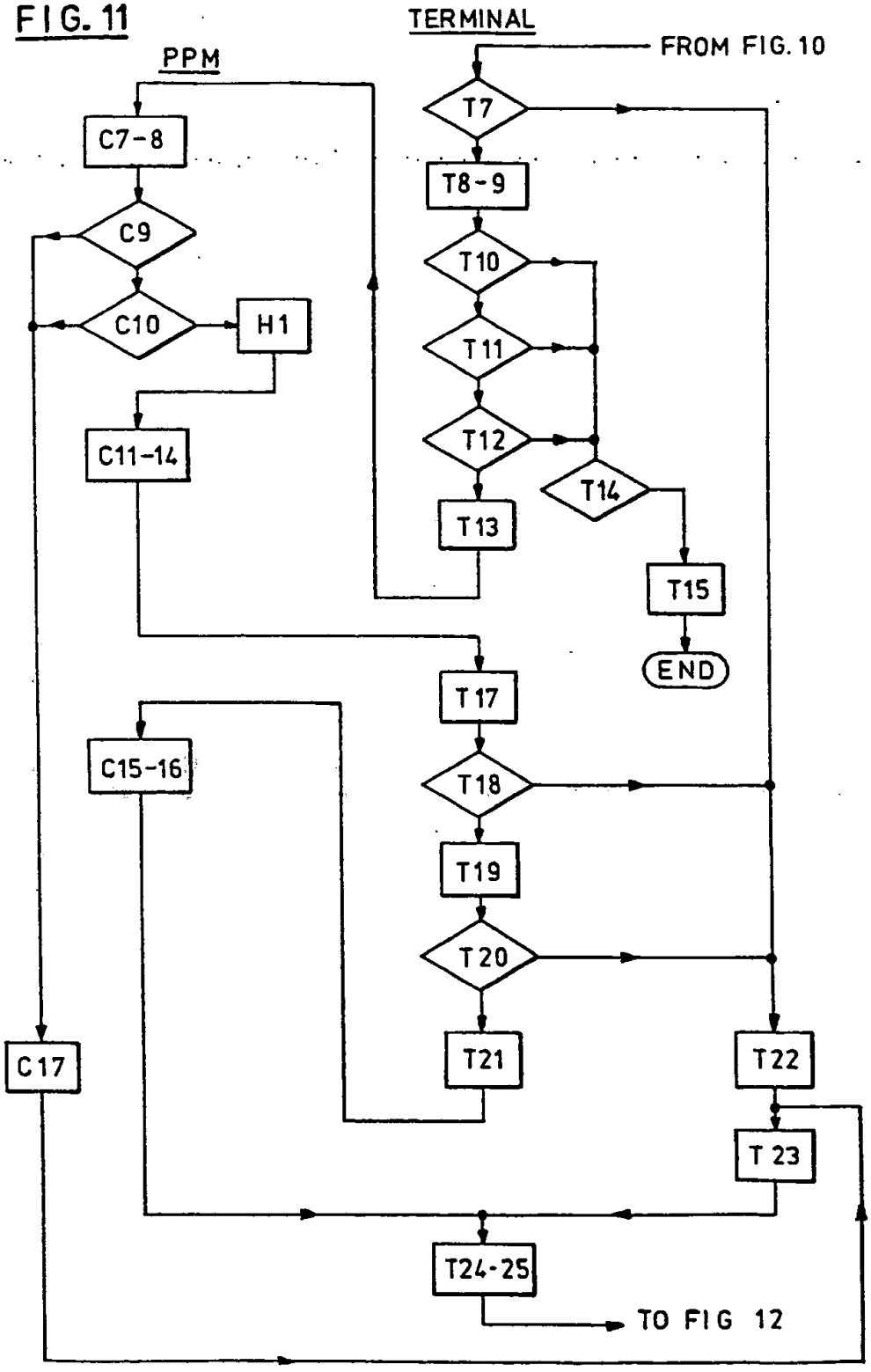

ISSUER HOST
SWITCH
ACQUIRER
TERMINAL
PPM
I1
I2
I3-7
I8
I9
I10-16
I17-19
S1
S2
S3-5
N1-2
N3-5
T1-4
T5-6
C1
C2-6
TO FIG.11

FIG. 10

FIG. 11


TERMINAL
FROM FIG. 10
PPM
T7
C7-8
T8-9
C9
T10
C10
H1
T11
C11-14
T12
T14
T13
T15
END
T17
C15-16
T18
T19
T20
C17
T21
T22
T23
T24-25
TO FIG 12

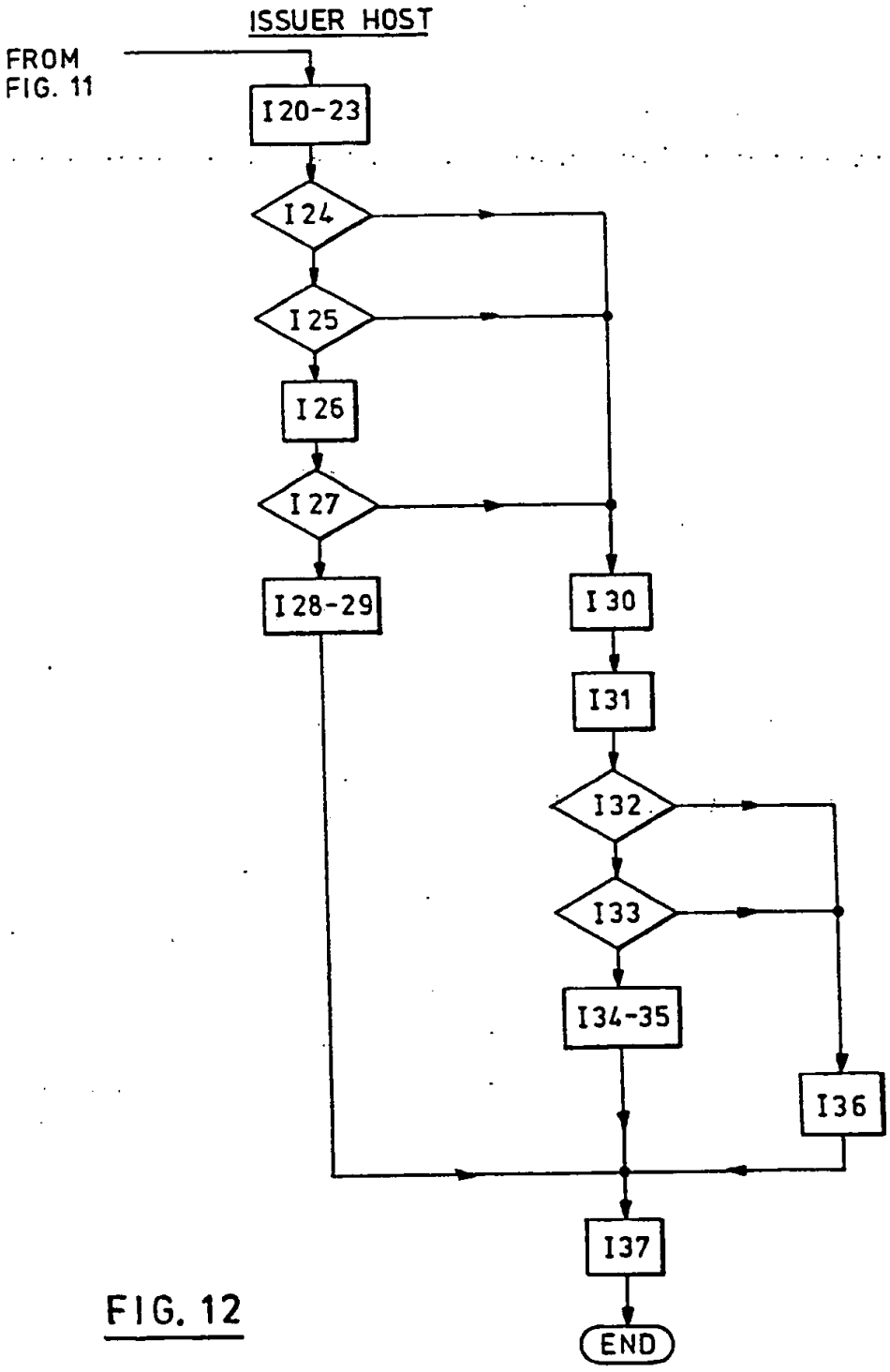

ISSUER HOST
FROM
FIG. 11
I20-23
I24
I25
I26
I27
I28-29
I30
I31
I32
I33
I34-35
I36
I37
END

FIG. 12

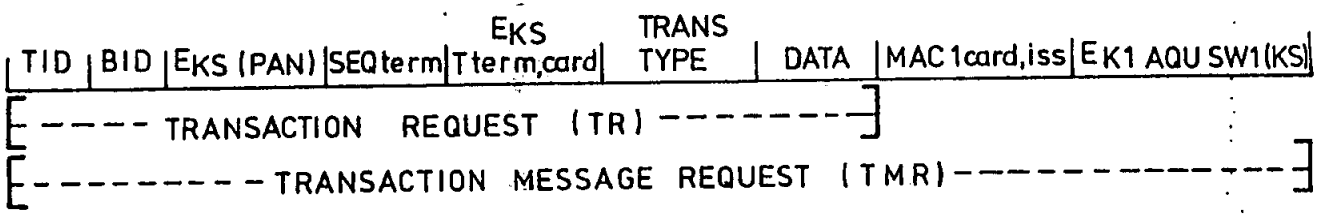


FIG. 13 MESSAGE REQUEST FORMAT

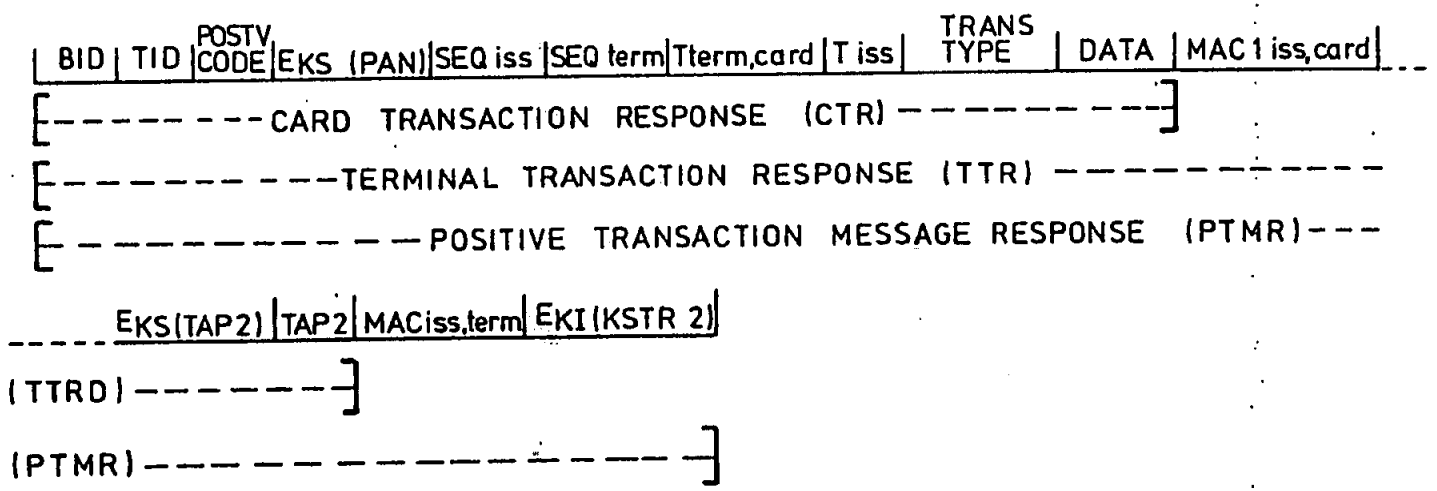


FIG 14 POSITIVE MESSAGE RESPONSE FORMAT

EP 0 140 013 B1

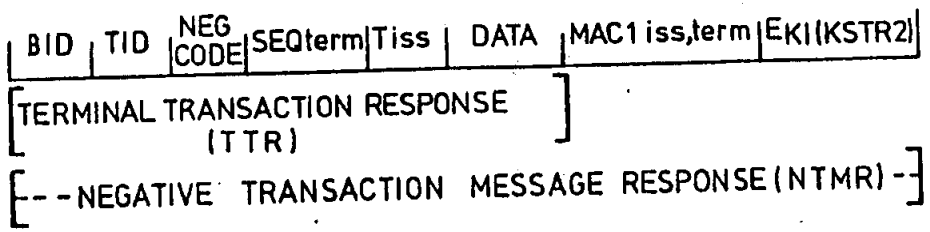


FIG. 15 NEGATIVE MESSAGE RESPONSE FORMAT

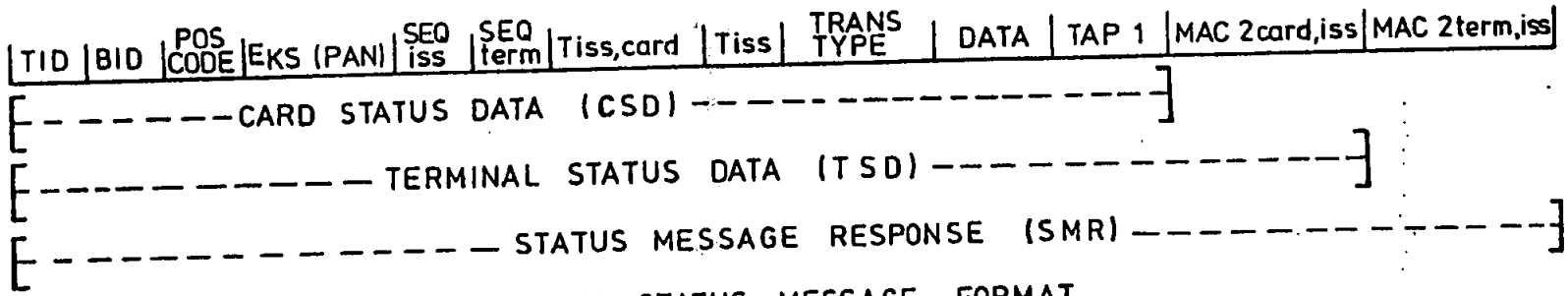


FIG. 16 TRANSACTION STATUS MESSAGE FORMAT

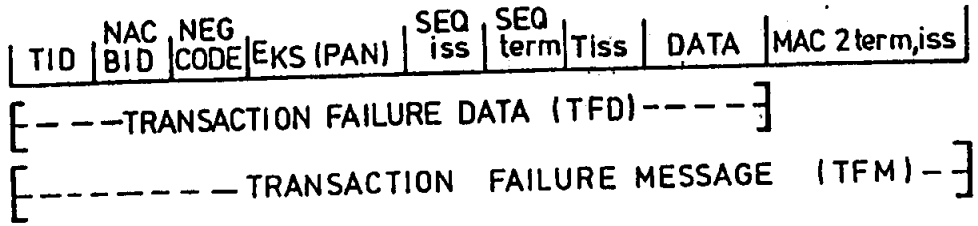


FIG. 17 NEGATIVE TRANSACTION STATUS MESSAGE FORMAT

EP 0 140 013 B1